DIGIPASS as a Service

Google Apps Integration

April 2011
# Table of Contents

## 1. Introduction
- 1.1. Audience and Purpose of this Document
- 1.2. Available Guides
- 1.3. What is DIGIPASS as a Service?
- 1.4. About VASCO

## 2. Prerequisites
- 2.1. Configuration by VASCO
- 2.2. Information Provided by VASCO

## 3. Google Apps Integration Setup
- 3.1. Overview
- 3.2. Downloading the DPS Certificate File
- 3.3. Configuring Google Apps for SAML with DPS
- 3.4. DPS User Configuration for use with Google Apps

## 4. Authenticating for a Google Application
- 4.1. Overview
- 4.2. Authenticating via the VASCO DPS Portal
- 4.3. Authenticating via the Google Apps server

## 5. Support
- 5.1. Overview
- 5.2. If you encounter a problem
- 5.3. Return procedure if you have a hardware failure
List of Figures

3.1. Downloading the DPS Certificate File
3.2. Google Apps Dashboard
3.3. Google Apps SSO Settings
3.4. SAML User Account
3.5. Accounts for Portal Tab
3.6. Account Policy
3.7. Account Credentials
3.8. Single Sign-On Account
3.9. Login of the 3rd party Application
4.1. Authentication via DPS Portal
**VASCO Products.** VASCO Data Security, Inc. and/or VASCO Data Security International GmbH are referred to in this document as ‘VASCO’. VASCO Products comprise Hardware, Software, Services and Documentation. This document addresses potential and existing VASCO customers and has been provided to you and your organization for the sole purpose of helping you to use and evaluate VASCO Products. As such, it does not constitute a license to use VASCO Software or a contractual agreement to use VASCO Products.

**Disclaimer of Warranties and Limitations of Liabilities.** VASCO Products are provided ‘as is’ without warranty or conditions of any kind, whether implied, statutory, or related to trade use or dealership, including but not limited to implied warranties of satisfactory quality, merchantability, title, non-infringement or fitness for a particular purpose. VASCO, VASCO DISTRIBUTORS, RESELLERS AND SUPPLIERS HAVE NO LIABILITY UNDER ANY CIRCUMSTANCES FOR ANY LOSS, DAMAGE OR EXPENSE INCURRED BY YOU, YOUR ORGANIZATION OR ANY THIRD PARTY (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF DATA) ARISING DIRECTLY OR INDIRECTLY FROM THE USE, OR INABILITY TO USE VASCO SOFTWARE, HARDWARE, SERVICES OR DOCUMENTATION, REGARDLESS OF THE CAUSE OF THE LOSS, INCLUDING NEGLIGENCE, EVEN IF VASCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR IF THEY WERE FORESEEABLE. OUR MAXIMUM AGGREGATE LIABILITY TO YOU, AND THAT OF OUR DISTRIBUTORS, RESELLERS AND SUPPLIERS SHALL NOT EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. THE LIMITATIONS IN THIS SECTION SHALL APPLY WHETHER OR NOT THE ALLEGED BREACH OR DEFAULT IS A BREACH OF A FUNDAMENTAL CONDITION OR TERM, OR A FUNDAMENTAL BREACH. THIS SECTION WILL NOT APPLY ONLY WHEN AND TO THE EXTENT THAT APPLICABLE LAW SPECIFICALLY REQUIRES LIABILITY DESPITE THE FOREGOING EXCLUSIONS AND LIMITATIONS.

**Intellectual Property and Copyright.** VASCO Products contain proprietary and confidential information. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights. No part of these Products may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted by VASCO or its authorized licensee in writing. This document is protected under US and international copyright law as an unpublished work of authorship. No part of it may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted in writing by VASCO or its authorized licensee.

**Trademarks.** VASCO®, VACMAN®, IDENTIKEY®, aXsGUARD™, DIGIPASS®, DIGIPASS as a Service™ and the ® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. Other company brand or product names or other designations, denominations, labels and/or other tags, titles, as well as all URLs (Internet addresses) linked to such designations or communications (irrespective of whether protected by intellectual property law or not), mentioned in VASCO Products may be the trademarks or registered trademarks or be part of any other entitlement of their respective owners.

**RADIUS Disclaimer.** Information on the RADIUS server provided in this document relates to its operation in the DIGIPASS as a Service environment. We recommend that you contact your NAS/RAS vendor for further information.

Copyright © 2011 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved.
Chapter 1. Introduction

1.1. Audience and Purpose of this Document

This document is intended for system administrators and technical experts who want to integrate DPS with (Google Apps). DPS provides Strong Authentication and Single Sign-On for Google Apps in a browser session. The authentication process on DPS uses the Security Assertion Markup Language (SAML) to communicate with the Google Apps servers. Users can authenticate for a Google Application directly via Google or via the DPS Portal.

This guide does not cover the steps to integrate the DIGIPASS for Web functionality. For information about DIGIPASS for Web, see your DIGIPASS for Web documentation which is included with the DIGIPASS for Web software.

In Section Chapter 2, Prerequisites, we explain important steps that must be taken before integrating DPS with your organisation’s Google Apps.

In section Chapter 3, Google Apps Integration Setup, we explain the configuration steps on the Google Apps Dashboard and on the DPS platform.

In section Chapter 4, Authenticating for a Google Application, we explain different methods to authenticate for a DPS-secured Google Application.

In section Chapter 5, Support, we explain how to request support.

Information about SAML is outside the scope of this manual. For information about SAML, see the DPS Proof of Concept Guide and the appropriate Internet resources.

1.2. Available Guides

The set of DPS documentation includes:

Conceptual documentation:

- **DPS Product Guide**, where we explain the concepts underpinning DPS and how DPS can provide authentication for your organisation’s online applications. This guide also provides the procedures to securely manage DPS resources, such as Users, Accounts, Authenticators, etc.
Howto guides:

- **DPS Web Administration Guide**, where we explain how to manage DPS Operators, Roles, Applications, Users and Authenticators via its web-based administration tool.
- **DPS REST Howto**, where we explain how to build REST API calls using HTTP CRUD operations.
- **DPS SOAP Howto**, where we explain how to build SOAP API calls.
- **DPS Google Apps Integration Guide**, where we explain how to integrate DPS Authentication with Google Apps.
- **DPS SalesForce Integration Guide**, where we explain how to integrate DPS Authentication with SalesForce.

Reference material:

- **DPS SOAP Reference Guide**, which is a technical reference document listing all available SOAP API calls.
- **DPS REST Reference Guide**, which lists all DPS Resources and how they can be addressed via REST.

All documents can be downloaded via the Web Administrator Tool’s **Help** function.

### 1.3. What is DIGIPASS as a Service?

DIGIPASS as a Service (DPS) is VASCO’s cloud-based authentication service platform which makes use of VASCO’s proprietary authentication technology. Organisations can secure their entire infrastructure via the DPS platform.

Nowadays, most web applications are secured with usernames and passwords, which can be easily hacked, stolen or passed on. Providers and customers have become more conscious about the security risk of static passwords and accelerate their investments in strong user authentication to protect their users’ business critical information.

B-to-B application owners sometimes face a number of barriers to the deployment of two-factor authentication for their user base. Sometimes they consider traditional strong authentication as too costly or they lack the resources to manage the distribution of authentication devices to end-users. As a result, VASCO experienced a strong demand from the market to launch DIGIPASS as a Service.

With DIGIPASS as a Service, VASCO is managing the full authentication process while the B-to-B provider focuses on its core business. The DIGIPASS as a Service offering includes a fully redundant hosted authentication back-end, the provisioning of DIGIPASS software or hardware authenticators to end-users, DIGIPASS services including fulfillment services (branding, customization, packaging, provisioning, distribution and storage), professional services and first line support.

### 1.4. About VASCO

VASCO is a world leader in strong authentication and e-signature solutions, specializing in online accounts, identities and transactions. As a global software company, VASCO serves a customer base of approximately 10,000 companies in over 100 countries, including approximately 1,500 international financial institutions. In addition to the financial sector, VASCO’s technologies secure
sensitive information and transactions for the enterprise security, e-commerce and e-government industries.

For further information, please visit http://www.vasco.com.
Chapter 2. Prerequisites

2.1. Configuration by VASCO

The following organisation-specific settings need to be configured by VASCO before DPS can be integrated by an organisation. The settings include the following items:

- **Organisation record**: This record contains organisation-specific information such as whether mutual authentication should be used or not.
- **Application records**: Are needed for each application secured by DPS.
- **Policies**: Authentication behavior is defined per application via Policies. For information about policies, see the DPS Policy guide (see Section 1.2, “Available Guides”)
- **DPX file**: Before Authenticators (e.g. DIGIPASS) can be used for authentication, the correct DPX file must be uploaded by VASCO.

Conceptual information about these items is available in the DPS Product guide (see Section 1.2, “Available Guides”).

2.2. Information Provided by VASCO

VASCO sends the following items to an organisation so it can log on to the DPS Web Administration Tool:

- An Operator Login.
- An Authenticator (e.g. a hardware DIGIPASS) to generate One-Time Passwords (OTP).
- Depending on the DIGIPASS type, a Static Password. The Static Password is only to be used if VASCO provided a DIGIPASS without Server PIN.

Practical information about accessing and using the DPS Web Administration Tool is available in the DPS Web Administration guide (see Section 1.2, “Available Guides”).
3.1. Overview

In this chapter we explain how to configure the Google Apps Dashboard. This step is required to secure the Google Apps, accessed from a given domain, with DPS.

Topics covered in this section include:

• How to download your DPS certificate file, needed for encryption and identification with Google Apps.
• How to activate and configure Google Apps on DPS and how to upload your certificate file.
• How to create User Accounts on DPS, so that Users can authenticate with their DPS user name and a One-Time password for a configured Google Application, rather than with an insecure static password.

3.2. Downloading the DPS Certificate File

In this section we explain how to download the DPS certificate file, which needs to be uploaded to Google via the Google Apps Control Panel. This certificate is signed by VASCO. It identifies and encrypts all authentication transactions between DPS and the Google Apps servers.

To download the DPS certificate file:

1. Log on to https://dps.vasco.com with a valid Operator Account, as explained in the Web Administration Guide.
2. Click on your organisation’s name in the upper left corner.
3. Select the Applications Tab.
4. Click on Portal.
5. Click on the Download certificate link.
6. Save the certificate file to the location of your choice.
For this procedure you need a Google Apps account. Information about obtaining a Google Apps account is available online. The following steps explain how to configure Google Apps for DPS integration:

**Accessing Advanced Tools**

1. Open a browser and log on to the Google Apps Dashboard
   

2. Click on Advanced Tools.

3. Click on Set up Single Sign-On (SSO).

**Single-Sign-On Settings**

2. In the field *Sign-in page URL*, insert the value from the App page in DPS, i.e. https://dps.vasco.com/portal/your_organisation_name/consume
3. In the *Sign-out URL* field, enter the URL as follows: https://dps.vasco.com/portal/your_organisation_name/consume
4. In the Change password URL fields, enter the URL as follows:
   https://dps.vasco.com/portal/your_organisation_name/dashboard
5. Locate and upload your DPS certificate file (see Section 3.2, “Downloading the DPS Certificate File”).
6. Save your changes.

This concludes the setup for Google Apps. You now have to create the correct User Accounts on DPS.

3.4. DPS User Configuration for use with Google Apps

For each Google Application Account, you must create two DPS User Accounts. There are two types of User Accounts on DPS:
• **Application Accounts**, which are needed to authenticate a User with DPS, e.g. Portal Accounts. An Authenticator, such as a hardware DIGIPASS, is assigned to this Account.

• **SAML Accounts**, which are Accounts to integrate SAML, e.g. for Google Apps or SalesForce. Such Accounts require a Login, but no Authenticator. The Login must be identical to the Login as known by the 3rd party application server, e.g. Google Apps or SalesForce. DPS passes this Login together with the Identity Assertion to the 3rd party application server when a User authenticates with his/her DPS Portal Account. The User remains authenticated for as long as the browser session established with DPS is valid.

If the Google Apps Account is for a new User, create the User first as explained in the Web Administration Guide.

Creating a SAML Account consists of two steps; creating a DPS Portal Account and creating a SAML integration Account.

**Create the DPS Portal Account**

1. Login to the DPS Web Administrator Tool as explained in the Web Administration Guide.
2. Click on the appropriate User Identifier as shown below.

   ![Figure 3.4. SAML User Account](image)

3. Click on the Accounts for Portal tab.

   ![Figure 3.5. Accounts for Portal Tab](image)

4. Select the appropriate Application Policy for the Login account, e.g. **Hardware Authenticator**. For information about Policies and their related work flows, see the DPS Policy Guide.
5. Enter a Login and enter the serial number of the Authenticator to be assigned.
6. Click on the Create button.

**Figure 3.6. Account Policy**

Create the SSO (SAML) Account on DPS

1. In the same tab, create a Single Sign-On Account.

**Figure 3.7. Account Credentials**

Create the SSO (SAML) Account on DPS

2. Enter the Login as known by the 3rd party application server, e.g. Google Apps or SalesForce.

**Figure 3.8. Single Sign-On Account**
3. Click on Create to finish.

During the transition phase, i.e. not all Users have received an Authenticator, a static password can be temporarily assigned for Authentication. Operators have to manually change this Policy once the User has received his/her Authenticator for the Application.
Chapter 4. Authenticating for a Google Application

4.1. Overview

In this chapter we explain how you can authenticate for a Google Application, once the DPS configuration as explained in Chapter 3, Google Apps Integration Setup has been completed. Users authenticate via a browser session.

There are 2 methods to authenticate for a Google Application, e.g. Gmail:

1. Users can authenticate directly via the DPS Portal with their DPS credentials (e.g. Login + DIGIPASS OTP) and select the Google Application.
2. Users can use the bookmarked URL of the Google Application. In that case the User is automatically redirected to the DPS Portal for authentication.

A User remains authenticated for as long as the browser session is valid. You need to sign out of the Google Application and the DPS Portal or close your browser to sign off completely.

4.2. Authenticating via the VASCO DPS Portal

To authenticate via the DPS Portal:

2. Enter your DPS credentials, e.g. your Account Login and your DIGIPASS OTP.
3. Click on Login.
4. Select the desired Google Application.
4.3. Authenticating via the Google Apps server

To authenticate via the Google Apps server:

1. Start a browser and enter the Google Apps server’s URL appended by the following string /a/dps.vasco.com/, e.g. https://mail.google.com/a/dps.vasco.com/.
2. Enter your DPS credentials, e.g. your Account Login and your DIGIPASS OTP.
3. Click on Login.

If you provided the correct credentials, you will have access to your Google Application.

Each Google Application is accessed via a different URL and requires you to register. See http://www.google.com/apps/ for additional information.
Chapter 5. Support

5.1. Overview
In this section we provide instructions on what to do if you have a problem, or experience a hardware failure.

5.2. If you encounter a problem
If you encounter a problem with a VASCO product, follow the steps below:

1. Check whether your problem has already been solved and reported in the Knowledge Base at the following URL: http://www.vasco.com/support
2. If there is no solution in the Knowledge Base, please contact the company which supplied you with the VASCO product.
3. If your supplier is unable to solve your problem, they will automatically contact the appropriate VASCO expert.

For details about support capabilities by user, visit: http://www.vasco.com/support/support_services/types_of_customes.aspx

5.3. Return procedure if you have a hardware failure
If you experience a hardware failure, contact your VASCO supplier.